



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/595,025	12/21/2005	Luis Barriga Caceres	P18155-US1	1351
27045	7590	07/09/2008	EXAMINER	
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR 1-C-11 PLANO, TX 75024			PHAM, LUU T	
			ART UNIT	PAPER NUMBER
			2137	
			MAIL DATE	DELIVERY MODE
			07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/595,025	Applicant(s) CACERES ET AL.	
	Examiner LUU PHAM	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) 1-24 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 24-46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 December 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/21/2005</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is in response to the application 10/595,025 filed on 12/21/2005.
2. As per the Preliminary Amendment filed on 12/21/2005, claims 1-23 were canceled; Claims 24-46 have been added. Claims 1-46 are pending in this application.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Claims 24-40 are rejected under 35 U.S.C. 101** as being directed to non-statutory subject matter.

- **Regarding claims 24 and 37**, the claims are not directed to eligible subject matter in view of *In re Comiskey*, 499 F.3d 1365 (Fed. Cir. 2007). The claims recite “*means for receiving the access credentials*,” “*means for checking validity*,” “*means for establishing a secure tunnel*,” “*means for assigning an internal IP address*,” “*means for establishing a secure tunnel*,” “*means for receiving an authentication challenge*,” and “*means for generating a public and private key pair*,” which do not require integrating a machine (e.g., a computer), or constitute a process of manufacture, or altering a composition of matter. There is no further disclosure in the specification as to how the aforementioned “*means for*” are implemented. Therefore, the nature of the subject matter claimed may reasonably be construed as a mental process since the language of claims 24 and 37 broadly encompasses non-tangible embodiments.

- **Regarding claims 25-36 and 38-40**, claims 25-26 and 38-40 are also directed to non-statutory subject matter for the same reasons.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claims 24-36 and 37-40 are rejected under 35 U.S.C. 112, second paragraph**, as being indefinite.

- **Regarding claims 24 and 37**, claims 24 and 37 have been found in valid as indefinite because the claims recite “*means for*” languages and there is no structure disclosed in the specification. “*If there is no structure in the specification corresponding to the means-plus-function limitation in the claims, the claims will be found invalid as indefinite.*” *Biomedino, LLC vs. Waters Technology Corp.*, 490 F.3d 946, 950 (Fed. Cir. 2007)

- **Regarding claims 25-36 and 38-40**, claims 25-26 and 38-40 are dependent on claims 24 and 37 respectively, and therefore inherit the 35 U.S.C 112, second paragraph issues of the independent claims.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted

on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. **Claim 37 is rejected under 35 U.S.C. 102(e)** as being anticipated by Jin et al., (hereinafter “Jin”), U.S. Patent No. 6,643,782, issued on November 04, 2003.

- **Regarding claim 37**, Jin teaches a user equipment arranged to carry out an authentication procedure with a core network, and arranged to access a telecommunication service network via an access network unable to provide data origin authentication (*col. 1, lines 15-21*), the user equipment, comprising:

means for obtaining access credentials as a result of being authenticated by the core network (*col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client*);

means for sending the access credentials towards the service network when accessing through the access network (*col. 2, lines 6-11; the NAS prepares and sends an ‘access-request’ packet to the AAA Server*);

means for establishing a secure tunnel with the service network through the access network, the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user (*col. 2, lines 40-59; the SSS Server is inserted between the NAS and AAA Server, and its function is to create secure channels to private areas of the network for authorized users*);

means for receiving an internal IP address assigned by the service network (*col. 2, lines 40-51; col. 5, lines 4-13 and 25-42*) and included as an inner IP address within the

tunnelled traffic to identify the user in the service network (*col. 2, lines 40-51; col. 5, lines 4-13 and 25-42; the SSG server checks for an IP address in the access-reply packet; the SSG Server can log the user on with the IP address provided by the AAA Server and then forward the access-reply packet on to the NAS*); and

means for linking said access credentials with the inner IP address and with the secure tunnel (*col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the user's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database*).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

11. **Claims 24-30 and 41-45 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Jin et al., (hereinafter “Jin”), U.S. Patent No. 6,643,782, issued on November 04, 2003, in view of Montenegro, U.S. Patent No. 6,571,289, issued on May 27, 2003.

- **Regarding claim 24**, Jin discloses an apparatus arranged for receiving a Single Sign-On service request in a telecommunication service network from a user via an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network (*col. 1, lines 15-21; the invention relates to a method for allowing single step log-on access to a network having more than one separate access area, such as a network divided into both public and private areas*), the apparatus comprising:

- means for receiving the access credentials from the user through the access network (*col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client*);

- means for checking validity of the access credentials received from the user (*col. 2, lines 23-30; the password entered by the user match the password specified in the account entry on the AAA database*);

- means for establishing a valid session with the user upon successful validity check of the access credentials (*col. 2, lines 44-46; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network*);

- means for assigning an internal IP address to identify the user in the service network (*col. 2, lines 40-46; col. 5, lines 3-7; in order for the network to communicate with*

the user, the user must be assigned an IP address; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network);

means for linking session data, access credentials and assigned internal IP address for the user (*col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the user's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database); and*

means for establishing a secure tunnel with the user when receiving the access credentials through the access network (*col. 2, lines 55-59; col. 5, lines 43-52; the SSG Server is inserted between the NAS and the AAA Server, and its function is to create secure channels to private areas of the network for authorized users)*

Jin does not explicitly disclose establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic.

However, in an analogous art, Montenegro disclose a method for negotiating access to a private network for a mobile node, wherein establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic (*col. 4, lines 20-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address of GW).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin wherein establishing a secure tunnel by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network as an inner IP address in the tunnelled traffic to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet (*col.2, lines 15-18*).

- **Regarding claim 25**, Jin and Montenegro disclose the apparatus of claim 24.

Jin further discloses means for generating service credentials for authorizing the user to access a service in the service network (*col. 1, lines 41-52; col. 2, lines 12-30*).

- **Regarding claim 26**, Jin and Montenegro disclose the apparatus of claim 25.

Jin further discloses the service credentials are generated on a per service basis for the user upon service request (*col. 2, lines 28-30; the access-accept packet contains configuration data that enable the NAS to provide the desired service to the user*).

- **Regarding claim 27**, Jin and Montenegro disclose the apparatus of claim 24.

Montenegro further discloses means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity (*col. 3, lines 31-65; the gateway 140 verifies an authentication which would accompany the registration request; the true home agent verifies the authentication for this registration and recognizes its validity*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include means for communicating with an Authentication Server of the home network in order to check the validity of the access credentials received from the user when said access credentials are not signed by a recognised authentication entity to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet (*col.2, lines 15-18*).

- **Regarding claim 28**, Jin and Montenegro disclose the apparatus of claim 24.

Jin further discloses the means for establishing the secure tunnel with the user are included in a first device named Secure Service Entry Point (*col. 1, lines 41-45, Network Access Server, NAS*), and the means for linking session data (*col. 2, lines 45-51*), access credentials and assigned internal IP address for the user are included in a second device named Single Sign-On Server (*col. 3, lines 25-53*).

- **Regarding claim 29**, Jin and Montenegro disclose the apparatus of claim 28.

Jin further discloses means for communicating the Secure Service Entry Point with the Single Sign-On Server (*col. 2, lines 52-59*).

- **Regarding claim 30**, Jin and Montenegro disclose the apparatus of claim 24.

Montenegro further discloses means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point for (*col. 3, lines 15-54; the FA 120 is the recipient of the registration request and since it will not be*

allowed to complete the registration request itself, unless the ISP were somehow given secure access, to the private network 150, the request is forwarded to the gateway 140).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin to include means for an additional co-ordination between the apparatus and an Identity Provider in charge of said user in a home network when said home network is different than the service network which the apparatus is the entry point to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet (*col.2, lines 15-18*).

- **Regarding claim 41**, Jin discloses a method for supporting Single Sign-On services in a telecommunication service network for a user accessing said service network through an access network unable to provide data origin authentication, the user having received access credentials as a result of being authenticated by a core network (*col. 1, lines 15-21; the invention relates to a method for allowing single step log-on access to a network having more than one separate access area, such as a network divided into both public and private areas*), the method comprising the steps of:

receiving at the service network the access credentials from the user through the access network (*col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client*);

checking validity of the access credentials received at the service network, establishing a valid session with the user upon successful validity check of the access

credentials (*col. 2, lines 23-30; the password entered by the user match the password specified in the account entry on the AAA database*);

assigning at the service network an internal IP address for the user to identify the user when accessing a service in the service network (*col. 2, lines 40-46; col. 5, lines 3-7; in order for the network to communicate with the user, the user must be assigned an IP address; once an IP address has been assigned to the user, the user is logged-on to the NAS and can begin his or her session on the network*);

linking session data, access credentials and the assigned internal IP address for the user at an entity of the service network (*col. 2, lines 40-51; col. 5, lines 25-42; after logging the user on, the NAS sends an "accounting-start" packet to the AAA Server, containing information regarding, for instance, the time at which the user's session begins, or other administrative and accounting data, that can be stored on the AAA Server's database*);

linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side (*col. 1, line 65-67 to col. 2, lines 1-9*).

Jin does not explicitly disclose establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network.

However, in an analogous art, Montenegro disclose a method for negotiating access to a private network for a mobile node, wherein establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by

using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network (*col. 4, lines 20-36; the address MN refers to the address of the mobile node when within the private network; the home agent will pre-pend an additional address of GW*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Montenegro with the method and system of Jin wherein establishing a secure tunnel between the user equipment side and an entity of the service network through the access network by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network to provide a mobile node with an ability to discover its intranet IP address even though it has migrated beyond the intranet (*col.2, lines 15-18*).

- **Regarding claims 42-45**, claim 42-45 are similar in scope to claims 25-28 respectively, and are therefore rejected under similar rationale.

12. **Claims 31-36 and 46 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Jin and Montenegro, as applied to claims 24 and 41 above, and further in view of Schneider et al., (hereinafter “Schneider”), U.S. Patent No. 6,105,027, issued on August 15, 2000.

- **Regarding claim 31**, Jin and Montenegro disclose the apparatus of claim 24.

Jin and Montenegro do not explicitly disclose the apparatus of claim 24 for use when the user is accessing a local HTTP service, or an external service in a network different

than the currently accessed service network, wherein the apparatus further comprises means for checking whether the user had been previously authenticated or not.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein the apparatus of claim 24 for use when the user is accessing a local HTTP service (*col. 43, lines 16-24; col. 45, lines 54-60; once the proxy has confirmed that access is to be allowed to the information resource specified in the message, the proxy originates a new session to the actual server, the HTTP service on server 407*), or an external service in a network different than the currently accessed service network, wherein the apparatus further comprises means for checking whether the user had been previously authenticated or not (*col. 48, lines 10-19; the other access filters between the user and the information item need only determine whether the request has already been authenticated by another access filter*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro to include means for checking whether the user had been previously authenticated or not in order to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 32**, Jin and Montenegro disclose the apparatus of claim 31.

Jin and Montenegro do not disclose means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network (*col. 26, lines 37-39; col. 40, lines 61-66; the service proxies intercept traffic for service such as the World Wide Web and do access checking on the traffic*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, to include means for communicating with an intermediate entity arranged to intercept the user's access to the HTTP local service, or to the external service in an external network in order to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 33**, Jin and Montenegro disclose the apparatus of claim 32.

Jin and Montenegro do not disclose the intermediate entity is an HTTP-proxy.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein the intermediate entity is an HTTP-proxy (*col. 40, lines 60-67; col. 3, lines 59-67*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein the intermediate entity is an HTTP-proxy to provide

users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 34**, Jin and Montenegro disclose the apparatus of claim 32.

Jin and Montenegro do not disclose the intermediate entity is a firewall.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein intermediate entity is a firewall (*col. 3, lines 59-67; access checking at the application is usually done in the firewall by proxies*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein intermediate entity is a firewall to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 35**, Jin and Montenegro disclose the apparatus of claim 24.

Jin and Montenegro do not disclose the apparatus of claim 24 for use when the user is accessing a non-HTTP local service, further having means for checking whether the user had been previously authenticated or not.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein the apparatus of claim 24 for use when the user is accessing a non-HTTP local service, further having means for checking whether the user had been previously authenticated or not (*col. 48, lines 10-19; the other access*

filters between the user and the information item need only determine whether the request has already been authenticated by another access filter).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, to include means for checking whether the user had been previously authenticated or not in order to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 36**, Jin and Montenegro disclose the apparatus of claim 24.

Jin and Montenegro do not disclose the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user (*col. 6, lines 12-16; col. 10, lines 11-54*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin and Montenegro, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user to provide users with a means for

speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 46**, claim 46 is similar scope to claim 31, and is therefore rejected under similar rationale.

13. **Claims 38-40 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Jin, as applied to claim 37 above, and further in view of Schneider et al., (hereinafter “Schneider”), U.S. Patent No. 6,105,027, issued on August 15, 2000.

- **Regarding claim 38**, Jin discloses the user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network (*col. 2, lines 16-30; the AAA Server receives an access-request packet from an authorized NAS client*);

means for generating and returning an authentication response to the core network (*col. 2, lines 16-39; if the passwords match, and all the other requirements are met, then the AAA Server send the NAS an “access-accept” packet in response; if nay requirement is not met, then the AAA Server responds with a “access-reject” packet*);

Jin does not explicitly disclose means for generating a public and private key pair; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising means for generating a public and

private key pair; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network (*col. 10, lines 19-27 and 59-61*);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin, to include means for generating a public and private key pair; and means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 39**, Jin discloses the user equipment of claim 37, wherein the means for obtaining access credentials includes:

means for receiving an authentication challenge from the core network (*col. 1, lines 65-67 to col. 2, lines 1-9*);

means for generating and returning an authentication response to the core network (*col. 1, lines 65-67 to col. 2, lines 1-9*); and

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising means for requesting a digital certificate obtainable from the core network (*col. 6, lines 12-17; col. 10, lines 11-42*);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin, to include means for requesting a digital certificate obtainable from the core

network to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

- **Regarding claim 40**, Jin discloses the user equipment of claim 39.

Jin does not explicitly disclose the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable.

However, in an analogous art, Schneider discloses a method for eliminating redundant access checking by access filter, comprising the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable (*col. 10, lines 11-54*);

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Schneider with the system and method of Jin, to include the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable to provide users with a means for speeding up access across a network by eliminating redundant access checking by access filters (*col. 5, lines 66-67 to col. 6, lines 1-20*).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent Publication No. US 2003/0229783 by Hardt.

U.S. Patent Publication No. US 2003/0171112 by Lupper et al.

U.S. Patent No. US 6,317,838 to Baize.

Art Unit: 2137

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137